

REMARKS

CLAIM REJECTIONS - 35 USC § 101

The Final Office action rejected claims 11-17 and 19-20 under 35 U.S.C. § 101 as not being limited to tangible embodiments. Applicant has amended paragraphs [0032] and [0081] of the specification to remove references to propagated signal transmissions (optical, wave, etc.). In light of these amendments, Applicant respectfully requests the rejection of these claims be withdrawn.

CLAIM REJECTIONS - 35 USC § 102

The Final Office action rejected claims 1-20 under 35 U.S.C. 102(e) as being anticipated by US Patent No. 6,401,208 issued to Davis et al. (*Davis*). Applicant submits claims 1-20 are not anticipated by *Davis* for at least the reasons set forth below.

Claims 1 and 11

Claim 1 is directed to a code module comprising code and a signature encrypted such that a computing device is capable of decrypting the signature using *a key embedded in a chipset* of the computing device. Claim 11, as amended, recites similar limitations.

The cited portion of *Davis* teaches a storage device 170 that contains BIOS code 180 and a digital BIOS certificate 181 and a BIOS signature 182. See column 3, lines 25-34. *Davis* further teaches that the BIOS signature 182 includes a digest of the BIOS code 180 signed by a private key of the BIOS vendor and that the BIOS certificate 181 includes a public key of the BIOS vendor signed by a private key of a certification authority. See column 3, lines 34-40. However, column 3, lines 6-40 of *Davis* **does not**

indicate how the digest of the BIOS signature 182 is decrypted and thus does not teach in the cited column 3, lines 6-40 a signature capable of being decrypted by an embedded key of a chipset, as recited in claims 1 and 11.

While the cited section of *Davis* does not teach how the digest of the BIOS signature is decrypted, other sections of *Davis* provide such information. In particular, *Davis* teaches pre-programming a cryptographic device 410 with a root certificate key 527. *Davis* column 5, lines 9-13. The cryptographic device 410 decrypts the BIOS certificate 181 using the root certificate key 527 of the cryptographic device 410 to obtain the public key of the signatory (e.g. BIOS vendor) of the BIOS signature 182. The cryptographic device 410 then uses the public key obtained from the BIOS certificate 181 to decrypt the digest of the BIOS signature 182. In sum, *Davis* appears to teach a storage device 170 that stores BIOS code 180, a BIOS certificate 181, and a BIOS signature 182 that is capable of being decrypted using ***a key of the BIOS certificate 181 stored in the storage device 170.***

The “Response to Arguments” section of the Final Office action acknowledges that the cryptographic device decrypts the BIOS certification using a root certificate key to retrieve the public key and that the public key is then used to recover (decrypt) the digest of the BIOS signature. Thus, the Final Office action implicitly acknowledges that the BIOS signature 182 is decrypted using a key of the BIOS certificate 181 stored in the storage device 170. FIG. 1 of *Davis* clearly shows the BIOS certificate 181 stored in device 170 and not in chipset 130. Thus, *Davis* does not appear to teach or disclose decrypting the signature using ***a key that is embedded in a chipset*** of the computing device, as claimed by Applicant. Therefore, Applicant respectfully submits claims 1 and

11 are not anticipated by *Davis*. Accordingly, Applicant respectfully requests the rejection of claim 1 and the rejection of claim 11 be withdrawn.

Claim 19

Claim 19 as amended is directed to machine readable medium comprising data pages, code pages, and a value encrypted such that a computing device is capable of decrypting the value *using an asymmetric key embedded in a chipset* of the computing device. As discussed above, *Davis* does not teach or disclose a value capable of being decrypted using a key embedded in a chipset. Accordingly, *Davis* does not appear to anticipate the invention of claim 19. Applicant respectfully requests the rejection of claim 19 be withdrawn.

Claims 4, 13 and 20

Each of claims 4, 13 and 20 includes a *SHA-1 hash* limitation. While *Davis* may disclose using a one-way hash, Applicant has been unable to locate where *Davis* teaches specifically using a SHA-1 hash as required by claims 4, 13 and 20. Without such a teaching, *Davis* does not anticipate the invention of claims 4, 13 and 20. Furthermore, claim 4 recites that the digest value is computed based upon a SHA-1 hash of the code *and the data*. Claims 13 and 20 similarly recites that the hash is of the code pages *and the data pages*. In contrast, *Davis* states, “[t]he BIOS *code* is read and undergoes the one-way hash function...” (emphasis added). Thus, the hash disclosed in *Davis* is only of the code and not of the code *and* the data as claimed by Applicant. Again, the failure of *Davis* to teach a limitation of the recited claims precludes *Davis* from anticipating the claims. Therefore, Applicant respectfully requests the rejection of claims 4, 13 and 20 be withdrawn.

Claims 6 and 14

Each of claims 6 and 14 require a field that identifies/specifies an execution point from which a computing device executes code. The Final Office action relies on column 4, lines 41-59 of *Davis* for such a teaching. As far as the Applicant can determine, *Davis* at column 4, lines 41-59 merely teaches that internal memory 525 contains firmware 526 which is a small computer program executed by first IC device 500. Column 4, lines 41-59 appears to provide no teaching regarding at what point or location execution of the firmware is to begin. Accordingly, *Davis* does not appear to teach a code module or a machine readable medium that has a field to identify/specify an execution point from which a computing device executes code.

The “Response to Arguments” section cites column 5, lines 9-32 of *Davis* to provide further support for the rejection of claims 6 and 14. This portion of *Davis* discusses delaying an instruction fetch until the cryptographic device has completed its internal initialization. There is no discussion of a code module or machine readable medium that has a field to identify/specify an execution point from which a computing device executes code. Given that *Davis* fails to teach at least one limitation of claims 6 and 14, Applicant respectfully submits *Davis* does not anticipate claims 6 and 14. Therefore, Applicant respectfully requests the present rejection of claims 6 and 14 be withdrawn.

Claims 7 and 15

Each of claims 7 and 15 require a marker that specifies the end of the code module (claim 7) or that specifies the end of the code pages and data pages (claim 15). The Final Office action relies on column 6, lines 20-30 of *Davis* for such a teaching.

Davis, however, at column 6, lines 20-30 appears to be silent in regard to a marker of a code module or a machine readable medium (See, FIG. 2 of Applicant's application) that specifies the end of a code module or the end of code pages and data pages.

Additionally, the "Response to Arguments" section of the Final Office action appears to equate a soft reset initiated by a predetermined signal from a predetermined signal line (column 6, lines 23-30) with a marker of a code module. Applicant fails comprehend the logic of comparing the activation of a signal line to a marker of a code module and the Final Office action offers no explanation for this comparison. Applicant contends that a signal is not equivalent to a marker and respectfully submits that the comparison is, therefore, erroneous.

For at least the reasons discussed above, Applicant submits claims 7 and 15 are not anticipated by *Davis*. Applicant respectfully requests the present rejection of claims 7 and 15 be withdrawn.

Claims 2, 3, 5, 8, 9, 10, 12, 16, 17 and 18

Each of claims 2, 3, 5, 8, 9, 10, 12, 16, 17 and 18 depends from one of claims 1 and 11. Accordingly, each of claims 2, 3, 5, 8, 9, 10, 12, 16, 17 and 18 is allowable for at least reasons stated above in regard to claims 1 and 11.

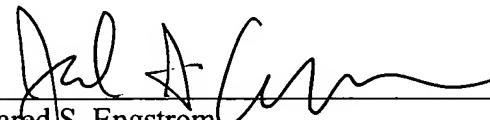
CONCLUSION

For at least the foregoing reasons, Applicant submits that the rejections have been overcome. Therefore, claims 1-20 are in condition for allowance and such action is earnestly solicited. The Examiner is respectfully requested to contact the undersigned by telephone if such contact would further the examination of the present application.

Please charge any shortages and credit any overcharges to our Deposit Account
number 02-2666.

Respectfully submitted,
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN, LLP

Date: 7/6/06



Jared S. Engstrom
Attorney for Applicant
Reg. No. 58,330

12400 Wilshire Boulevard
Seventh Floor
Los Angeles, CA 90025-1026
(503) 439-8778

I hereby certify that this correspondence is being deposited with
the United States Postal Service as first class mail with sufficient
postage in an envelope addressed to Commissioner for Patents,
P.O. Box 1450, Alexandria, VA 22313 on:

7/6/06

Date of Deposit
Annie Pearson

Name of Person Mailing Correspondence
Annie Pearson

Signature 7/6/06 Date